NICEWG Workforce Management Charter

Vision:

Each individual in an organization is fulfilling their specific responsibilities to understand and mitigate cybersecurity risks.

Mission:

Facilitate, develop and promote cybersecurity workforce management guidance and measurement approaches that create a culture where the workforce is managed and engaged to effectively address the cybersecurity risks of their organization.

Objectives:

1. Support the ongoing effort to update the NICE Cybersecurity Workforce Framework so that it remains current and relevant for stakeholders.
2. Produce recommendations and guidelines for developing a cybersecurity culture focused on organizational and individual and role-based responsibilities, leadership involvement, and behavioral change.
3. Establish a consensus on promising, sustainable practices directed at an organization for improved management, collaboration and decision making to better engage all individuals in understanding and performing their cybersecurity risk-management responsibilities.
4. Describe strategies and general planning considerations to support organizations in implementing the recommendations and guidance developed by the Workforce Management subgroup.
5. Identify deliverables and timelines for specific products that will support the Workforce Management subgroup's vision and can be incorporated into the appropriate NICE efforts.
6. Collaborate with NICE Working Groups (K-12, Collegiate, Competitions, Training and Certifications) and national workforce development efforts to communicate workforce management needs.

Short-Term Deliverables:

(Project teams currently working)

- Integrate human elements of enterprise risk management with the NIST Cybersecurity Framework (CSF), NICE Workforce Framework and other applicable constructs in order to provide a broader, more comprehensive set of guidelines for enterprise cybersecurity.
- Develop structure, role profiles and core "knowledge areas" used to map KSAs to certifications, roles and academic CBE classes.

- Inventory and assess existing research and literature; to include frameworks, maturity models, practices, data and analysis, relevant to creating a cybersecurity workforce culture where the workforce is managed and engaged to effectively address their cybersecurity risk responsibilities.

Long-Term Deliverables:

(Potential work for future project teams)

- Create a template for a Cybersecurity Workforce (CSW) Program Plan and supporting documents for agencies to use to develop, document and manage their CSW Program.
- Create a template for organizations to use to develop and publish a workforce gap analysis in accordance with the Federal Cybersecurity Workforce Assessment Act of 2015
- Identify additional gaps in cyber-related workforce management
- Communicate evidence for successful models for improvements in standard human resource practice to enhance the cybersecurity talent lifecycle
- Develop guidance, metrics, and templates to help agencies formulate effective Cybersecurity Talent strategies aligned with the organization's risk management strategy and industry standards; publish a report on identifying, analyzing, recording, and managing workforce-related cybersecurity risks
- Develop guidelines for creating a cybersecurity culture focused on organizational and individual responsibilities, leadership involvement, behavioral change approaches, and compliance enforcement mechanisms
- Develop models for cybersecurity organizational structures and incentives to improve collaboration and decision making regarding risk management within agencies